Forensic Science International 262 (2016) 242–275

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

Review Article

An evolution of image source camera attribution approaches

Mehdi Jahanirad *, Ainuddin Wahid Abdul Wahab, Nor Badrul Anuar **

Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 14 July 2015
Received in revised form 12 March 2016
Accepted 16 March 2016
Available online 22 March 2016

Keywords:
Camera attribution
Image feature
Image forensics
Image processing
Image mining

ABSTRACT

Camera attribution plays an important role in digital image forensics by providing the evidence and distinguishing characteristics of the origin of the digital image. It allows the forensic analyser to find the possible source camera which captured the image under investigation. However, in real-world applications, these approaches have faced many challenges due to the large set of multimedia data publicly available through photo sharing and social network sites, captured with uncontrolled conditions and undergone variety of hardware and software post-processing operations. Moreover, the legal system only accepts the forensic analysis of the digital image evidence if the applied camera attribution techniques are unbiased, reliable, nondestructive and widely accepted by the experts in the field. The aim of this paper is to investigate the evolutionary trend of image source camera attribution approaches from fundamental to practice, in particular, with the application of image processing and data mining techniques. Extracting implicit knowledge from images using intrinsic image artifacts for source camera attribution requires a structured image mining process. In this paper, we attempt to provide an introductory tutorial on the image processing pipeline, to determine the general classification of the features corresponding to different components for source camera attribution. The article also reviews techniques of the source camera attribution more comprehensively in the domain of the image forensics in conjunction with the presentation of classifying ongoing developments within the specified area. The classification of the existing source camera attribution approaches is presented based on the specific parameters, such as colour image processing pipeline, hardware- and software-related artifacts and the methods to extract such artifacts. The more recent source camera attribution approaches, which have not yet gained sufficient attention among image forensics researchers, are also critically analysed and further categorised into four different classes, namely, optical aberrations based, sensor camera fingerprints based, processing statistics based and processing regularities based, to present a classification. Furthermore, this paper aims to investigate the challenging problems, and the proposed strategies of such schemes based on the suggested taxonomy to plot an evolution of the source camera attribution approaches with respect to the subjective optimisation criteria over the last decade. The optimisation criteria were determined based on the strategies proposed to increase the detection accuracy, robustness and computational efficiency of source camera brand, model or device attribution.

Contents

* Corresponding author. Tel.: +60 129790054.
** Corresponding author. Tel.: +60 123201147.
E-mail addresses: mehdijahanirad@siswa.um.edu.my (M. Jahanirad), ainuddin@um.edu.my (A.W.A. Wahab), badrul@um.edu.my (N.B. Anuar).

http://dx.doi.org/10.1016/j.forsciint.2016.03.035
0379-0738/

1. Introduction

Today's digital cameras store the image metadata along with the image itself on DVDs, CD-ROMs, and media cards. The image file metadata (i.e. extended file information header (EXIF)) includes data about the image such as the make and model of the camera, the date and time the image was captured, the focal length and shutter stops. If a forensic examination is conducted only on a computer, and images captured by a digital camera are discovered, the metadata within the image files can be used to link them back to a specific camera. However, EXIF headers are less reliable because the information in the EXIF metadata is easily editable through software like ExifTool, or it could be lost if the image file format is changed, for example, due to software processing applied on images prior to their upload, transfer and download through the photo sharing or social network sites. Having this limitation, camera attribution is among the most studied areas in image forensics because it helps to identify the source of a digital image. This is also known as forensic characterisation of digital cameras, which means identifying the type, make, model, configuration, and other characteristics of the camera device through analysis of the image that it has captured [48].

The image source camera attribution research community has achieved substantial advances, especially in recent years. Nevertheless, it is difficult to standardise digital image forensics for court room consideration due to the rapid growth and ever changing challenges of the computer field. New products are emerging constantly and commonly used forensic tools may not be able to handle certain items properly, or even at all, at the time when an examination is needed [91]. This paper is an attempt to investigate the camera attribution problem, including its potential advantages, challenging aspects, existing methodologies, and recent advances. Particularly, discussion of the existing camera attribution methods has been conducted pertaining to the different artifacts of the colour image processing pipeline. Using a similar approach, prior works have also considered the video processing artifacts for source video camera attribution [95,96]. However, for this study, the image forensics investigation was narrowed down to image source camera attribution approaches in an attempt to concentrate more on the classification of image artifacts and the methods to extract such artifacts; meanwhile, it studies each method with respect to specific challenging aspects addressed. Moreover, we present existing issues related to real-time camera attribution in practice, and discuss future directions of research in this area.

Digital image forensics have been addressed in several reviews on digital forensics: In [113,126,127] and a survey of forensics characterisation methods for physical devices [130]. The more specific surveys and reviews on digital image forensics are as follows: short review of limited source digital camera attribution and forgery detection approaches [133]; classification of digital image forensics to three branches, including image source attribution, discrimination of synthetic images and image forgery detection [134]; study of the trends and challenges in digital image and video forensics, including the main topic areas of source camera attribution, forgery detection and steganalysis [135]; a comprehensive collected book on theoretical aspects of digital image forensics [91], which covers the methods for creation, processing and storing of digital images, describes the latest techniques for forensically examining images, and addresses practical issues such as courtroom admissibility; a booklet, including the detail overview of the existing tools for image source device attribution and tampering detection [136]; a comprehensive classification on image forgery detection techniques [138]. Despite the extensive reviews in digital image forensics, limited works have addressed an in-depth study to the source camera attribution techniques. Due to growing number of publications in this field, there remains a need for an efficient study that can perform a new, precise and crisp classification among these approaches, to explain the differences and identify current gaps and challenges in this field. This paper aims to discuss an evolution of the research with a generic and comprehensive